The Retail Solution v. 12.0 PA-DSS Secure Implementation Guide Version 1.1

Northwest Network Solutions, Inc.

Revision History

Version Number	Release Date	Author/Reviewer	Description
1.0	03/31/2014	Carol Clark	Initial Draft
1.1	04/07/14	Carol Clark	Release

This implementation guide is reviewed at least annually and updated when changes to software and/or PA-DSS requirements occur.

Table of Contents

About PCI Security Standards

The PCI-DSS (Payment Card Industry Data Security Standard) is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical measures to protect customer account data. All businesses handling credit and debit cards are required by the card brands to maintain PCI-DSS compliance.

There are 12 basic requirements for PCI compliancy, which can be grouped into 6 categories. Following is a brief review of these requirements with Retail Solution-specific guidelines. However, you are responsible for knowing and meeting the PCI standards. For more information, and to download detailed PCI requirements documentation, visit http://www.pcisecuritystandards.org

Category 1: Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

- You should have a firewall at each internet connection, between any wireless network and computers on which cardholder data is stored and between computers on which cardholder data is stored and the network as a whole.
- Each firewall should be securely configured with stateful inspection to allow only business-necessary traffic.
- You must document your firewall configuration and review it on a regular basis to verify that it meets PCI standards.
- Any computer which stores cardholder data should be segregated from the rest of your network, as well as from public access. For example, the computer on which your Retail Solution data resides should not be located on a server that hosts email or websites.

Requirement 2: Do not use vendor-supplied defaults for system passwords, default encryption keys, SNMP community strings and other security parameters. All defaults should be changed on installation.

- This requirement applies not just to The Retail Solution, but to all aspects of your system, including network administration, firewalls and routers, wireless devices, remote access software, etc. In addition, these settings should be changed anytime someone with knowledge of them leaves the company or changes positions.
- **If you are using The Retail Solution 12.0 with our demo data**, credit card payment processing features are disabled. When you select the "Go Live" option to begin entering your live data, the default demo data password "DEMO" will be disabled. You will be prompted to enter employee information, including unique user ID and enhanced password, for the administrator.
- **If you upgrade from a version prior to 11.0**, you will be required to assign both a login name and password to each employee. Verify that the "Administrative Privileges" option on the Privileges tab is selected only for authorized employees. An employee with administrative privileges, and/or with access to Employee Information, is required to have an enhanced password (p. 9). Once you have verified that employee logins/passwords/access rights are correct, select "Activate advanced security" from the Options menu at the Employee Information window.

Category 2: Protect Cardholder Data

Requirement 3: Protect stored cardholder data.
Credit card information should only be entered at the payment screen when completing a sale in the PowerStation. The Retail Solution can optionally store credit card number and expiration date for future or recurring charges.This information is encrypted at the station level using advanced encryption technology. Do not enter credit card information anywhere else in the program (for example, in customer notes, or as a comment on an invoice.)

By default the option to store credit card information for future use is turned off. If you elect to turn this feature on, credit card information will be stored based on the "number of months invoice history is saved" setting on the Point-of-Sales Options tab in Company Information, or the card expiration date, whichever is greater. Card information is securely deleted during the End-of-Month procedure. You should run the End-of-Day procedure on a regular basis, the End-of-Month procedure at the end of each calendar month, and the End-of-Year procedure at the end of your fiscal year. To securely delete all credit card numbers from your database immediately, de-select the option to store credit card information for future sales. An individual credit card number can be deleted at the Customer Information window.

Stored credit card numbers can only be viewed by a designated administrative user. Refer to the Manager's Workstation Help topic, "Enhanced Passwords" for information on creating an administrative user. A stored credit card number can be viewed in the following places:

- At the Customer Information window, on the User Info tab, by clicking on the "No." label under the credit card type name.
- At the point-of-sale, by clicking the credit card icon next to the customer name.
- When viewing payment information for a completed ticket, by clicking the field under "Ask First".

PCI requirements prohibit storage of the following, in any format: full contents of the magnetic stripe track, card validation code (CAV2/CVC2/CVV2/CID), and/or PIN number/PIN block. Previous versions of The Retail Solution may have stored sensitive data. When you upgrade your data with version 12.0, this information is automatically and securely deleted. It is essential that you securely delete or destroy data backups from previous versions. You should also verify that you are not storing full, unencrypted card numbers or other prohibited information in your paper records.

The Retail Solution 12.0 does not use or store sensitive card data for troubleshooting purposes. If you need to store such information briefly in order to solve a specific problem, you are responsible for meeting PCI security requirements, including storing only the minimum data required, storing data only in a specific, known location with limited access, encrypting data while stored, and securely deleting data as soon as it is no longer needed.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.
The Retail Solution encrypts card data at the station level using AES 256 bits CTR with a dynamic key encryption. However, you are responsible for the encryption and secure transmission of

information (using industry best practices, such as IEEE 802.11.i) when using remote connections, wireless devices, email, websites, etc. Cardholder information (including credit card number, cardholder name, expiration date, and service code) should never transmitted electronically in an unencrypted format (for example, via email, instant messaging, or chat.) Any wireless devices with access to cardholder data should be configured with the strongest encryption technology currently available.

Category 3: Maintain a Vulnerability Management Program

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs.
Anti-virus software should be implemented on all components of your network. Verify that you are protected against all types of malicious software, including viruses, worms, Trojans, etc. Anti-virus software should be frequently updated and software logs reviewed regularly.

Requirement 6: Develop and maintain secure systems and applications.
You are responsible to keep your system updated with the latest security patches for your operating system, The Retail Solution, and other components of your system. If you are using PC Charge, ICVerify, or X-Charge software, you must verify that the version you are using is PCI-compliant, and that you obtain, review, and follow the software's PA-DSS Secure Implementation Guide. If you are using a PIN Pad device, you must verify that your device is PCI-compliant.

The Retail Solution Versioning System
- **Maintenance updates** to the current version are indicated by build number. For example, Version 12.0 build 15.
- **Security-related updates** are indicated by the format [Version number].[Update number]. For example, Version 12.1

Category 4: Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know.
In The Retail Solution, access to stored credit card information is only available to an administrative level user. An administrative user is any user with access to employee information and/or with the administration privilege selected on the Privileges tab in Employee Information. This user is required to have a unique ID and **strong password**. (A strong password must be at least 7 characters, must include both numbers and letters, must be changed every 90 days, and cannot be the same as the last 4 passwords.) If a user no longer needs access to the system, (for example, an employee is terminated), their status should be changed to "inactive" in Employee Information, and their password will be disabled.

Requirement 8: Identify and authenticate access to system components.
Each user must have a unique login name and password. Do not use group, shared or generic accounts and passwords. This applies not only to The Retail Solution, but to your computer system as a whole, including firewalls/routers, operating systems, wireless devices, etc.

If you do not want the user's login name displayed anywhere in the program, select **"Hide login name"** on the Miscellaneous tab in Company Information.

In The Retail Solution, if an incorrect password is entered more than 5 times in a row, that login name will be locked out for 15 minutes. If no other valid logins are made within that 15 minutes, and then another wrong password is entered, that login name will be locked out permanently until the lock is turned off by an administrative user.

The Retail Solution does not require use of remote access software. If you choose to use remote access software, you are responsible to meet PCI security guidelines, including the following:
- Change default settings in the remote-access software (for example, change default passwords and use unique passwords for each customer).
- Allow connections only from specific (known) IP/MAC addresses.
- Use strong authentication and complex passwords for logins.
- Enable encrypted data transmission
- Enable account lockout after a certain number of failed login attempts
- Establish a Virtual Private Network (VPN) connection via a firewall before access is allowed.
- Enable the logging function.
- Restrict access to customer environments to authorized integrator/reseller personnel.

Requirement 9: Restrict physical access to cardholder data.
Physical access to your computer system, including data backups, should be carefully monitored and limited to authorized personnel.

To enhance security in the PowerStation, select the option "At the end of each sale, lock the register" on the Point-of-Sale Options tab in Company Information.

Category 5: Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.
You are responsible to maintain an audit trail for all components of your computer system. The Retail Solution automatically tracks login access. An administrative user should regularly check and monitor this log. This information can be viewed in The Manager's Workstation on the Audit tab at the Employee Information window. This information cannot be edited by any user.

The Retail Solution's employee logs can be exported to a centralized logging server by creating a report with the report source "Employee Transaction Logs". After running the report, select the "Export" option.

Requirement 11: Regularly test security systems and processes.
This is especially important after any change to the system, such as installation of new software/hardware or software upgrades.

Category 6: Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors.

You should develop a formal information security policy which includes a regular risk review process, and includes employee training on security requirements.

Glossary

AES: Abbreviation for Advanced Encryption Standard.

Authentication: Process of verifying identity of an individual, device or process.

Cardholder Data: Credit card number, with or without the following additional information: Cardholder name, expiration date, and service code.

Card Verification Code or Value: Security code included in the magnetic stripe or printed on the card. Also known as CVC, CVV, CSC, CID, CVC2, CVV2.

Default Password: Predefined password on system administration or service accounts for a system, application, or device, usually associated with a default accounts.

Encryption: Process of converting data into a coded format which cannot be read without use of the code key.

Firewall: Hardware or software that prevents unauthorized access to network resources.

Host: Main computer on which software resides.

Magnetic Stripe Data: Data encoded in a credit card's magnetic stripe or chip, used for card authorization during a payment transaction.

PIN: Abbreviation for "Personal Identification Number". Secret numeric password known only to the user and the card authentication system.

Router: Hardware or software that connects two or more networks. Sorts and routs data to correct locations.

SSH: Abbreviation for "Secure Shell". Protocol suite providing encryption fort network services like remote login or remote file transfer.

SSL: Acronym for "Secure Socket Layer". Established industry standard that encrypts the channel between a web browser and web server to ensure the privacy and reliability of data transmitted over this channel.

Stateful Inspection: Also known as "Dynamic Packet Filtering". A firewall capability that provides enhanced security by monitoring communications packets and blocking unauthorized incoming packets.

Strong cryptography: Cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key-management practices. Includes both encryption and hashing. Examples include SHA-1 (hashing) and AES128 or greater (encryption).

TLS: Acronym for "Transport Layer Security". Designed with the goal of providing data secrecy and integrity between two communicating applications.

Two-Factor Authentication: Method of authenticating a user in which two or more factors are verified. These factors include something the user has (such as a hardware or software token), something the user knows (such as a password, passphrase, or PIN) or something the user is or does (such as fingerprints or other forms of biometrics).

VPN: Acronym for "Virtual Private Network". A computer network in which some connections are virtual circuits within a larger network, such as the Internet, instead of a direct physical connection. Web Server: Computer that contains a program that accepts HTTP requests from web clients and serves the HTTP responses (usually web pages).